Text Part Number: 78-5563-04

Release Notes for Cisco 2500 Series for Cisco IOS Release 12.0 T

May 3, 1999

These release notes describe new features and significant software components for the Cisco 2500 series that support Cisco IOS Release 12.0 T, up to and including Release 12.0(4)T. These release notes are updated as needed to describe new memory requirements, new features, new hardware support, software platform deferrals, microcode or modem code changes, related document changes, and any other important changes.

For a list of the software caveats that apply to Release 12.0(4)T, refer to the *Caveats for Cisco IOS Release 12.0 T* document that accompanies these release notes. The caveats document is updated for every maintenance release and is located on Cisco Connection Online (CCO) and the Documentation CD-ROM.

Use these release notes with the *Cross-Platform* R*elease Notes for Cisco IOS Release 12.0 T* located on CCO and the Documentation CD-ROM.

Contents

These release notes discuss the following topics:

- System Requirements, page 2
- New and Changed Information, page 14
- Important Notes, page 28
- Caveats, page 35
- Related Documentation, page 35
- Service and Support, page 39
- Cisco Connection Online, page 40
- Documentation CD-ROM, page 41

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA

Copyright © 1998–99
Cisco Systems, Inc.
All rights reserved.

System Requirements

This section describes the system requirements for Release 12.0 T and includes the following sections:

- Memory Requirements, page 2
- Hardware Supported, page 3
- Determining Your Software Release, page 4
- Upgrading to a New Software Release, page 4
- Feature Set Tables, page 4

Memory Requirements

Table 1 Memory Requirements for Cisco 2500 Series Routers

Platforms	Feature Sets[1]	Image Name	Software Image	Required Flash Memory	Required DRAM Memory	Runs from	In[2]
Cisco 2500 Series	IP Feature Sets	IP	c2500-i-l	8 MB	6 MB	Flash	
		IP/FW	c2500-io-l	8 MB	6[4] MB	Flash	
		IP/FW Plus IPSec 56	c2500-ios56i-l	16 MB	8 MB	Flash	
		IP Plus	c2500-is-l	16[3] MB	4 MB	Flash	
		IP Plus 40	c2500-is40-l	16[3] MB	4 MB	Flash	
		IP Plus 56	c2500-is56-l	16[3] MB	6[4] MB	Flash	
		IP Plus IPSec 56	c2500-is56i-l	16 MB	6[4] MB	Flash	
		IP/H323	c2500-ix-l	8 MB	16 MB	Flash	(4)
		IP/IBM/APPN	c2500-ai3r4-l	16 MB	8 MB	Flash	
		IP/IPX/AT/DEC	c2500-d-l	8 MB	4 MB	Flash	
		IP/IPX/AT/DEC/FW Plus	c2500-dos-l	16 MB	6[4] MB	Flash	
		IP/IPX/AT/DEC Plus	c2500-ds-l	16 MB	4[5] MB	Flash	
	Enterprise Feature Sets	Enterprise/APPN Plus IPSec 56	c2500-ajs56i-l	16 MB	8 MB	Flash	
		Enterprise/FW Plus IPSec 56	c2500-jos56i-l	16 MB	8 MB	Flash	
		Enterprise Plus	c2500-js-l	16 MB	6[3] MB	Flash	
		Enterprise Plus IPSec 56	c2500-js56i-l	16 MB	8 MB	Flash	
	FRAD Feature Sets	FRAD	c2500-f-l	8 MB	6[4] MB	Flash	
		LAN FRAD/OSPF	c2500-f2in-l	8 MB	6[4] MB	Flash	
		LAN FRAD	c2500-fin-l	8 MB	6[4] MB	Flash	
		Remote Access Server (RAS)	c2500-c-l	8 MB	4[5] MB	Flash	
		ISDN	c2500-g-l	8 MB	6[4] MB	Flash	

1 If you need to upgrade the main memory for your Cisco series router, be sure to order the upgrade specific to your router.

2 The number in the “In” column indicates the Cisco IOS release when the image was first introduced. For example, (4) means an image was introduced in Release 12.0(4)T. If a cell in this column is empty, the interface was included in the initial base release.

3 8 MB in Releases 12.0(1)T, 12.0(2)T, and 12.0(3)T.

4 4 MB in Releases 12.0(1)T, 12.0(2)T, and 12.0(3)T.
5 6 MB in Releases 12.0(1)T, 12.0(2)T, and 12.0(3)T.

Hardware Supported

Cisco IOS Release 12.0 T supports the Cisco 2500 series:

- Single LAN routers—Models 2502, 2503, 2504, 2520, 2521, 2522 and 2523
- Mission-specific, entry-level routers—Models 2501CF, 2502CF, 2503I, 2504I, 2520CF, 2520LF, 2521CF, 2521LF, 2522CF, 2522LF, 2523CF and 2523LF
- Router/hub combinations—Models 2505, 2507 and 2516
- Access servers—Models 2509 to 2512
- Dual LAN routers—Models 2513, 2514 and 2515
- Modular routers—Models 2524 and 2525 (optional integrated DSU/CSU or NT-1)

For detailed descriptions of the new hardware features, refer to the "New and Changed Information" section on page 14.

Table 2 Supported Interfaces for the Cisco 2500 Series

Interface, Network Module, or Data Rate	Product Description	Platforms Supported
LAN Interfaces	Ethernet (AUI)	Cisco 2501, 2503, 2509, 2511, 2513, 2514, 2520, 2522, and 2524 only
	Ethernet (10BaseT)	Cisco 2505, 2507, 2516, and 2524 only
	4-Mbps Token Ring	Cisco 2502, 2504, 2513, 2515, 2521, 2523, and 2525 only
	16-Mbps Token Ring	Cisco 2502, 2504, 2513, 2515, 2521, 2523, and 2525 only)
WAN Data Rates	48/56/64 kbps	Cisco 2500 series
	128 kbps	Cisco 2500 series
	1.544/2.048 Mbps	Cisco 2500 series
WAN Interfaces	EIA/TIA-232	Cisco 2500 series
	EIA/TIA-449	Cisco 2500 series
	EIA-530	Cisco 2500 series
	X.21	Cisco 2500 series
	V.35	Cisco 2500 series
	Serial, synchronous	Cisco 2500 series
	Serial, synchronous, and asynchronous	Cisco 2520, 2521, 2522, and 2523 only
	ISDN BRI S/T	Cisco 2503, 2504, 2516, 2520, 2521, 2522, 2523, 2524, and 2525 only
	ISDN BRI U	Cisco 2524 and 2525 only

Cisco AS2509-RJ and Cisco AS2511-RJ Access Servers

The Cisco AS2509-RJ and Cisco AS2511-RJ access servers connect asynchronous serial devices to LANs and WANs. The access servers combine the functions of a terminal server, protocol translator, and a router and perform both synchronous and asynchronous routing of supported protocols.

These access servers provide the following interfaces and ports:

- Eight (Cisco AS2509-RJ) or 16 (Cisco AS2511-RJ) asynchronous serial ports for connection to modems, terminals, or other asynchronous devices
- One Ethernet attachment unit interface (AUI) port for connection to a LAN
- One synchronous serial port for connection to a WAN
- One EIA/TIA-232 console port for connection to a console terminal
- One EIA/TIA-232 auxiliary port for connection to a terminal or modem

Determining Your Software Release

To determine the version of Cisco IOS software currently running on your Cisco 2500 series router, log in to the platform and enter the **show version** EXEC command. The following sample output from the **show version** command indicates the version number on the second output line:

```
router>show version
Cisco Internetwork Operating System Software
IOS (tm) 2500 Software (C2500-DOS-L), Version 12.0(4)T, RELEASE SOFTWARE
```

Additional command output lines include more information, such as processor revision numbers, memory amounts, hardware IDs, and partition information.

Upgrading to a New Software Release

For information on upgrading to a new software release, refer to the *Cisco IOS Software Release 12.0 T Upgrade Paths and Packaging Simplification (#819: 1/99)* product bulletin located on CCO.

On CCO, click on this path:

Service & Support: Product Bulletins: Software

Under **Cisco IOS 12.0**, click **Cisco IOS Software Release 12.0 T Upgrade (#819: 1/99)**.

Feature Set Tables

The Cisco IOS software is packaged in feature sets consisting of software images—depending on the platform. Each feature set contains a specific set of Cisco IOS features.

Release 12.0 T supports the same feature sets as Release 12.0, but Release 12.0 T can include new features supported by the Cisco 2500 series.

Table 3 Feature Sets Supported by the Cisco 2500 Series

Feature Set Image Names	Feature Set Matrix Term	Software Image	Platforms	In[1]
IP	Basic	c2500-i-l	Cisco 2500 series	
IP/FW	Basic	c2500-io-l	Cisco 2500 series	

Table 3 Feature Sets Supported by the Cisco 2500 Series (continued)

Feature Set Image Names	Feature Set Matrix Term	Software Image	Platforms	In[1]
IP/FW Plus IPSec 56	Plus, IPSec 56	c2500-ios56i-l	Cisco 2500 series	
IP Plus	Plus	c2500-is-l	Cisco 2500 series	
IP Plus 40	Plus 40	c2500-is40-l	Cisco 2500 series	
IP Plus 56	Plus 56	c2500-is56-l	Cisco 2500 series	
IP Plus IPSec 56	Plus, IPSec 56	c2500-is56i-l	Cisco 2500 series	
IP/H323	Basic	c2500-ix-l	Cisco 2500 series	(4)
IP/IBM/APPN	Basic	c2500-ai3r4-l	Cisco 2500 series	
IP/IPX/AT/DEC	Basic	c2500-d-l	Cisco 2500 series	
IP/IPX/AT/DEC/FW Plus	Plus	c2500-dos-l	Cisco 2500 series	
IP/IPX/AT/DEC Plus	Plus	c2500-ds-l	Cisco 2500 series	
Enterprise/APPN Plus IPSec 56	Plus, IPSec 56	c2500-ajs56i-l	Cisco 2500 series	
Enterprise/FW Plus IPSec 56	Plus, IPSec 56	c2500-jos56i-l	Cisco 2500 series	
Enterprise Plus	Plus	c2500-js-l	Cisco 2500 series	
Enterprise Plus IPSec 56	Plus, IPSec 56	c2500-js56i-l	Cisco 2500 series	
FRAD	Basic	c2500-f-l	Cisco 2501, 2502, Cisco 2520–2523	
LAN FRAD/OSPF	Basic	c2500-f2in-l	Cisco 2501, 2502, Cisco 2520–2523	
LAN FRAD	Basic	c2500-fin-l	Cisco 2501, 2502, Cisco 2520–2523	
Remote Access Server (RAS)	Basic	c2500-c-l	Cisco 2500 series	
ISDN	Basic	c2500-g-l	Cisco 2500 series	

1 The number in the “In” column indicates the Cisco IOS release when the image was first introduced. For example, (4) means an image was introduced in Release 12.0(4)T. If a cell in this column is empty, the interface was included in the initial base release.

Caution Cisco IOS images with strong encryption (including, but not limited to, 56-bit data encryption feature sets) are subject to United States government export controls and have a limited distribution. Images to be installed outside the United States require an export license. Customer orders may be denied or subject to delay because of United States government regulations. Contact your sales representative or distributor for more information, or send an e-mail to export@cisco.com.

Table 4, Table 5, and Table 6 list the features and feature sets supported by the Cisco 2500 routers in Cisco IOS Release 12.0 T. All three tables use the following conventions:

- Yes—The feature is supported in the software image.
- No—The feature is not supported in the software image.

- In—The number in the "In" column indicates the Cisco IOS release in which the feature was first introduced. For example, (4) means a feature was introduced in Release 12.0(4)T. If a cell in this column is empty, the feature was included in the initial base release.

Note These feature set tables only contains a selected list of features. These tables are not cumulative— nor do they list all the features in each image.

Table 4 Feature List by Feature Set for the Cisco 2500 Series, Part 1

		Feature Sets						
Features	**In**	**IP**	**IP/FW**	**IP/FW Plus IPSec 56**	**IP Plus**	**IP Plus 40**	**IP Plus 56**	**IP Plus IPSec 56**
IBM Support								
Bridging Code Rework		Yes	Yes	Yes	Yes	Yes	Yes	Yes
DLSw+ Enhancements	(3)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
RIF Passthru in DLSw+		No	No	No	Yes	Yes	Yes	Yes
IP Routing								
Easy IP Phase 2-DHCP Server	(1)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Flow WRED	(3)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
IP Type of Service and Precedence for GRE Tunnels		Yes	Yes	No	Yes	Yes	Yes	Yes
OSPF Point to Multipoint		Yes	Yes	Yes	Yes	Yes	Yes	Yes
OSPF Packet Pacing	(1)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Protocol-Independent Multicasts (PIM) Version 2		Yes	Yes	Yes	Yes	Yes	Yes	Yes
WCCP v2 Support	(3)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
X.25 Load Balancing	(3)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Management								
Cisco IOS File System		Yes	Yes	Yes	Yes	Yes	Yes	Yes
Conditionally Triggered Debugging		Yes	Yes	Yes	Yes	Yes	Yes	Yes
Entity MIB		Yes	Yes	Yes	Yes	Yes	Yes	Yes
Expression MIB		Yes	Yes	Yes	Yes	Yes	Yes	Yes
ISDN MIB RFC 2127	(1)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Migration of Distributed Director	(3)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Process MIB	(3)	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Table 4 Feature List by Feature Set for the Cisco 2500 Series, Part 1 (continued)

	Feature Sets							
Features	**In**	**IP**	**IP/FW**	**IP/FW Plus IPSec 56**	**IP Plus**	**IP Plus 40**	**IP Plus 56**	**IP Plus IPSec 56**
Response Time Reporter Enhancements	(3)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SNMP Manager		Yes	Yes	Yes	Yes	Yes	Yes	Yes
SNMP v3	(3)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Scalability								
Airline Product Set (ALPS)		Yes	Yes	Yes	Yes	Yes	Yes	Yes
ALPS II - UTS Support	(1)	No	No	Yes	Yes	Yes	Yes	Yes
Security								
AAA Support for MS-CHAP		No	No	No	No	No	No	No
Additional Vendor-Proprietary RADIUS Attributes		Yes	Yes	Yes	Yes	Yes	Yes	Yes
Authenticating ACL		Yes	Yes	Yes	Yes	Yes	Yes	Yes
Automated Double Authentication		No	Yes	Yes	Yes	Yes	Yes	Yes
Context-Based Access Control (CBAC)		No	No	Yes	No	No	No	No
Certificate Authority Interoperability		No	No	No	No	No	No	Yes
Internet Key Exchange Security Protocol		No	No	No	No	No	No	Yes
IPSec Network Security		No	No	No	No	No	No	Yes
Named Method Lists for AAA Authentication & Accounting		Yes	Yes	Yes	Yes	Yes	Yes	Yes
WAN Optimization								
DRP Server Agent Enhancements		Yes	Yes	Yes	Yes	Yes	Yes	Yes
WAN Services								
Always On Dynamic ISDN		No	No	No	No	No	No	No
Annex G	(3)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Async over UDP	(3)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Dialer Watch		Yes	Yes	Yes	Yes	Yes	Yes	Yes

Table 4 Feature List by Feature Set for the Cisco 2500 Series, Part 1 (continued)

		Feature Sets						
Features	**In**	**IP**	**IP/FW**	**IP/FW Plus IPSec 56**	**IP Plus**	**IP Plus 40**	**IP Plus 56**	**IP Plus IPSec 56**
Dynamic Multiple Encapsulations for Dial-in over ISDN	(4)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Mobile IP	(1)	No	No	Yes	Yes	Yes	Yes	Yes
MPPC- MS PPP Compression		Yes	Yes	Yes	Yes	Yes	Yes	Yes
MS Callback		Yes	Yes	Yes	Yes	Yes	Yes	Yes
Multiple ISDN Switch Types		Yes	Yes	Yes	Yes	Yes	Yes	Yes
National ISDN Switch Type		Yes	Yes	Yes	Yes	Yes	Yes	Yes
PPP Over Frame Relay	(1)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Time-Based Access Lists	(1)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
VPDN MIB Feature		No	No	No	Yes	Yes	Yes	Yes
Quality of Service								
CLI Search String	(1)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Parse Bookmarks	(1)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Switching								
Cisco IOS STP Enhancements	(1)	No	No	Yes	Yes	Yes	Yes	Yes
Connectivity								
RIP Enhancements	(1)	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Table 5 Feature List by Feature Set for the Cisco 2500 Series, Part 2

		Feature Sets						
Features	**In**	**IP/H.323**	**IP/IBM/ APPN**	**IP/IPX/AT/ DEC**	**IP/IPX/AT/ DEC/ FW Plus**	**IP/IPX/AT/ DEC Plus**	**Enterprise /APPN Plus IPSec 56**	**Enterprise /FW Plus IPSec 56**
IBM Support								
Bridging Code Rework		Yes	Yes	Yes	Yes	Yes	Yes	Yes
DLSw+ Enhancements	(3)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
RIF Passthru in DLSw+		Yes	Yes	No	No	Yes	Yes	Yes

Table 5 Feature List by Feature Set for the Cisco 2500 Series, Part 2 (continued)

	Feature Sets							
Features	**In**	**IP/H.323**	**IP/IBM/ APPN**	**IP/IPX/AT/ DEC**	**IP/IPX/AT/ DEC/ FW Plus**	**IP/IPX/AT/ DEC Plus**	**Enterprise /APPN Plus IPSec 56**	**Enterprise /FW Plus IPSec 56**
IP Routing								
Easy IP Phase 2-DHCP Server	(1)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Flow WRED	(3)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
IP Type of Service and Precedence for GRE Tunnels		Yes	Yes	Yes	Yes	Yes	Yes	Yes
OSPF Point to Multipoint		Yes	Yes	Yes	Yes	Yes	Yes	Yes
OSPF Packet Pacing	(1)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Protocol-Independent Multicasts (PIM) Version 2		Yes	Yes	Yes	Yes	Yes	Yes	Yes
WCCP v2 Support	(3)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
X.25 Load Balancing	(3)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Management							Yes	
Cisco IOS File System		Yes	Yes	Yes	Yes	Yes		Yes
Conditionally Triggered Debugging		Yes	Yes	Yes	Yes	Yes	Yes	Yes
Entity MIB		Yes	Yes	Yes	Yes	Yes	Yes	Yes
Expression MIB		Yes	Yes	Yes	Yes	Yes	Yes	Yes
ISDN MIB RFC 2127	(1)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Migration of Distributed Director	(3)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Process MIB	(3)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Response Time Reporter Enhancements	(3)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SNMP Manager		Yes	Yes	Yes	Yes	Yes	Yes	Yes
SNMP v3	(3)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Scalability							Yes	
Airline Product Set (ALPS)		Yes	No	Yes	Yes	Yes		Yes
ALPS II - UTS Support	(1)	Yes	No	No	Yes	Yes	Yes	Yes
Security							Yes	
AAA Support for MS-CHAP		Yes	No	No	No	No	Yes	Yes

Table 5 Feature List by Feature Set for the Cisco 2500 Series, Part 2 (continued)

		Feature Sets						
Features	**In**	**IP/H.323**	**IP/IBM/ APPN**	**IP/IPX/AT/ DEC**	**IP/IPX/AT/ DEC/ FW Plus**	**IP/IPX/AT/ DEC Plus**	**Enterprise /APPN Plus IPSec 56**	**Enterprise /FW Plus IPSec 56**
Additional Vendor-Proprietary RADIUS Attributes		Yes	Yes	Yes	Yes	Yes	Yes	Yes
Authenticating ACL		Yes	Yes	No	Yes	Yes	No	Yes
Automated Double Authentication		Yes	Yes	Yes	Yes	Yes	Yes	Yes
Context-Based Access Control (CBAC)		Yes	No	No	No	Yes	Yes	No
Certificate Authority Interoperability		Yes	No	No	No	No	Yes	Yes
Internet Key Exchange Security Protocol		Yes	No	No	No	No	Yes	Yes
IPSec Network Security		Yes	No	No	No	No	Yes	Yes
Named Method Lists for AAA Authentication & Accounting		Yes	Yes	Yes	Yes	Yes	Yes	Yes
WAN Optimization								
DRP Server Agent Enhancements		Yes	No	No	Yes	Yes	Yes	Yes
WAN Services								
Always On Dynamic ISDN		Yes	No	No	No	No	Yes	Yes
Annex G	(3)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Async over UDP	(3)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Dialer Watch		Yes	Yes	Yes	Yes	Yes	Yes	Yes
Dynamic Multiple Encapsulations for Dial-in over ISDN	(4)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Mobile IP	(1)	Yes	No	No	Yes	Yes	Yes	Yes
MPPC- MS PPP Compression		Yes	Yes	Yes	Yes	Yes	Yes	Yes
MS Callback		Yes	Yes	Yes	Yes	Yes	Yes	Yes
Multiple ISDN Switch Types		Yes	Yes	No	Yes	Yes	Yes	Yes
National ISDN Switch Type		Yes	Yes	No	Yes	Yes	Yes	Yes

Table 5 Feature List by Feature Set for the Cisco 2500 Series, Part 2 (continued)

		Feature Sets						
Features	**In**	**IP/H.323**	**IP/IBM/ APPN**	**IP/IPX/AT/ DEC**	**IP/IPX/AT/ DEC/ FW Plus**	**IP/IPX/AT/ DEC Plus**	**Enterprise /APPN Plus IPSec 56**	**Enterprise /FW Plus IPSec 56**
PPP Over Frame Relay	(1)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Time-Based Access Lists	(1)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
VPDN MIB Feature		Yes	No	Yes	No	Yes	Yes	Yes
Quality of Service								
CLI Search String	(1)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Parse Bookmarks	(1)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Switching								
Cisco IOS STP Enhancements	(1)	Yes	Yes	No	Yes	Yes	Yes	Yes
Connectivity								
RIP Enhancements	(1)	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Table 6 Feature List by Feature Set for the Cisco 2500 Series, Part 3

		Feature Set						
Features	**In**	**Enterprise Plus**	**Enterprise Plus IPSec 56**	**FRAD**	**LAN/ FRAD/ OSPF**	**LAN/ FRAD**	**Remote Access Server**	**ISDN**
IBM Support								
Bridging Code Rework		Yes	Yes	Yes	Yes	Yes	No	Yes
DLSw+ Enhancements	(3)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
RIF Passthru in DLSw+		Yes	Yes	Yes	Yes	Yes	No	Yes
IP Routing								
Easy IP Phase 2-DHCP Server	(1)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Flow WRED	(3)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
IP Type of Service and Precedence for GRE Tunnels		Yes	Yes	No	No	No	Yes	Yes
OSPF Point to Multipoint		Yes	Yes	Yes	Yes	Yes	Yes	Yes
OSPF Packet Pacing	(1)	Yes	Yes	Yes	No	No	No	Yes

Table 6 Feature List by Feature Set for the Cisco 2500 Series, Part 3 (continued)

Features	In	Feature Set: Enterprise Plus	Enterprise Plus IPSec 56	FRAD	LAN/ FRAD/ OSPF	LAN/ FRAD	Remote Access Server	ISDN
Protocol-Independent Multicasts (PIM) Version 2		Yes	Yes	Yes	No	No	No	No
WCCP v2 Support	(3)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
X.25 Load Balancing	(3)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Management								
Cisco IOS File System		Yes	Yes	Yes	Yes	Yes	Yes	Yes
Conditionally Triggered Debugging		Yes	Yes	Yes	Yes	Yes	Yes	Yes
Entity MIB		Yes	Yes	Yes	Yes	Yes	Yes	Yes
Expression MIB		Yes	Yes	Yes	Yes	Yes	Yes	Yes
ISDN MIB RFC 2127	(1)	Yes	Yes	No	No	No	No	Yes
Migration of Distributed Director	(3)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Process MIB	(3)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Response Time Reporter Enhancements	(3)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SNMP Manager		Yes	Yes	Yes	Yes	Yes	Yes	Yes
SNMP v3	(3)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Scalability								
Airline Product Set (ALPS)		Yes	Yes	Yes	Yes	Yes	Yes	Yes
ALPS II - UTS Support	(1)	Yes	Yes	No	No	No	No	No
Security								
AAA Support for MS-CHAP		Yes	Yes	No	No	No	No	No
Additional Vendor-Proprietary RADIUS Attributes		Yes	Yes	Yes	Yes	Yes	No	Yes
Authenticating ACL		Yes	Yes	Yes	No	No	No	No
Automated Double Authentication		Yes	Yes	Yes	No	No	No	No
Context-Based Access Control (CBAC)		No	No	No	No	No	No	No

Table 6 Feature List by Feature Set for the Cisco 2500 Series, Part 3 (continued)

Features	In	Feature Set: Enterprise Plus	Enterprise Plus IPSec 56	FRAD	LAN/ FRAD/ OSPF	LAN/ FRAD	Remote Access Server	ISDN
Certificate Authority Interoperability		No	Yes	No	No	No	No	No
Internet Key Exchange Security Protocol		No	Yes	No	No	No	No	No
IPSec Network Security		No	Yes	No	No	No	No	No
Named Method Lists for AAA Authentication & Accounting		Yes	Yes	Yes	Yes	Yes	Yes	Yes
WAN Optimization								
DRP Server Agent Enhancements		Yes	Yes	Yes	No	No	No	No
WAN Services								
Always On Dynamic ISDN		Yes	Yes	No	No	No	No	No
Annex G	(3)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Async over UDP	(3)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Dialer Watch		Yes	Yes	Yes	Yes	Yes	Yes	Yes
Dynamic Multiple Encapsulations for Dial-in over ISDN	(4)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Mobile IP	(1)	Yes	Yes	No	No	No	No	No
MPPC- MS PPP Compression		Yes	Yes	Yes	Yes	Yes	No	Yes
MS Callback		Yes	Yes	Yes	Yes	Yes	Yes	Yes
Multiple ISDN Switch Types		Yes	Yes	Yes	No	No	Yes	No
National ISDN Switch Type		Yes	Yes	Yes	No	No	Yes	No
PPP Over Frame Relay	(1)	Yes	Yes	Yes	Yes	Yes	Yes	No
Time-Based Access Lists	(1)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
VPDN MIB Feature		Yes	Yes	Yes	No	No	Yes	No
Quality of Service								
CLI Search String	(1)	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Table 6 Feature List by Feature Set for the Cisco 2500 Series, Part 3 (continued)

	Feature Set							
Features	**In**	**Enterprise Plus**	**Enterprise Plus IPSec 56**	**FRAD**	**LAN/ FRAD/ OSPF**	**LAN/ FRAD**	**Remote Access Server**	**ISDN**
Parse Bookmarks	(1)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Switching								
Cisco IOS STP Enhancements	(1)	Yes	Yes	Yes	Yes	Yes	No	No
Connectivity								
RIP Enhancements	(1)	Yes	Yes	Yes	Yes	Yes	Yes	Yes

New and Changed Information

The following sections list the new hardware and software features supported by the Cisco 2500 series in Release 12.0 T.

New Software Features in Release 12.0(4)T

The following new software enhancements are supported by the Cisco 2500 series in Release 12.0(4)T.

One New Feature Set

One new feature set has been created for the Cisco 2500 series in Release 12.0(4)T:

- IP/H.323—c2500-ix-l

Dynamic Multiple Encapsulations for Dial-in over ISDN

The Dynamic Multiple Encapsulations feature allows incoming calls over Integrated Services Digital Network (ISDN) to be assigned an encapsulation type such as Point-to-Point Protocol (PPP), X.25, and ISDN Link Access Procedure, Balanced-Terminal Adapter (LAPB-TA) based on calling line identification (CLID) or Dialed Number Identification Service (DNIS). It also allows various encapsulation types as well as per-user configurations on the same ISDN B channel at different times according to the type of incoming call.

The Dynamic Multiple Encapsulations feature allows per-user configuration for each dial-in caller on any ingress ISDN B channel on which encapsulation can be run independently from other B channels on the same ISDN link. The caller is identified by CLID or DNIS to make sure that only incoming calls with authorization and valid user profiles are accepted. If the protocol is PPP, authentication and profile binding can also be done by PPP name.

Dynamic multiple encapsulations are especially important in Europe where ISDN is relatively inexpensive, and it is desirable to allow maximum use of all B channels on the same ISDN link, especially for large scale dial-in. Further, the feature removes the need to statically dedicate channels to a particular encapsulation and configuration type, and improves channel usage.

Although the Dynamic Multiple Encapsulations feature enhances large scale dial-in functionality, the feature also works well in smaller scale dial-in situations and for modem calls.

New Software Features in Release 12.0(3)T

The following new software enhancements are supported by the Cisco 2500 series in Release 12.0(3)T.

Annex-G (X.25 over Frame Relay)

Annex G (X.25 over Frame Relay) facilitates the migration from an X.25 backbone to a Frame Relay backbone by permitting encapsulation of CCITT X.25/X.75 traffic within a Frame Relay connection. Annex G has developed to accommodate the many Cisco customers in Europe, where X.25 still is a popular protocol. With Annex G, the process of transporting X.25 over Frame Relay has been simplified, by allowing direct X.25 encapsulation over a Frame Relay network.

This simple process is largely achieved using X.25 profiles (similar to dialer profiles), which were created to streamline the configuration of X.25 on a per DLCI basis. X.25 profiles can contain any existing X.25 command and, once created and named, can be simultaneously associated with more than one Annex G DLCI connection, just using the profile name.

CDP Additions for Cisco IOS

The Cisco Discovery Protocol (CDP) is a media-independent device discovery protocol that runs on all cisco manufactured equipment, including routers, bridges, access servers, and switches. Each device sends periodic messages to a multicast address. Each device listens to the periodic messages sent by others in order to learn about neighboring devices and determine when their interfaces to the media go up or down. With CDP, network management applications can learn the device type and the SNMP agent address of neighboring devices. This process enables applications to send SNMP queries to neighboring devices.

CDP runs on all media that support Subnetwork Access Protocol (SNAP), including local-area network (LAN), Frame Relay, and Asynchronous Transfer Mode (ATM) media. CDP runs over the data link layer only. Therefore, two systems that support different network-layer protocols can learn about each other.

Each device configured for CDP sends periodic messages to a multicast address. Each device advertises at least one address at which it can receive SNMP messages. The advertisements also contain time-to-live, or holdtime, information, which indicates the time a receiving device should hold CDP information before discarding it.

Additions for Cisco Discovery Protocol (CDP) include the following:

- new SYSLOG output for instances of mismatching native VLAN IDs (IEEE 802.1Q) on connecting ports and port duplex state values on connecting devices.
- **cdp advertise-v2** command and new output from **show cdp** commands

The benefits include, transparent support of X.25 encapsulation over the Frame Relay network; direct X.25 configurations on a per DLCI basis; multiple Annex G DLCIs can use the same X.25 profile; multiple logical X.25 SVCs per Annex G link, and the fact that Cisco routers already contain the functionality necessary to perform the framing and frame removal required by Annex G.

Cisco Multipath Channel+ (CMPC+)

Cisco Multipath Channel+ (CMPC+) is Cisco's implementation of IBM's MPC+ feature. The CMPC+ feature in Cisco IOS Release 12.0(3)T supports MPC+ features and protocols necessary to support IP. CMPC+ enables High Performance Data Transfer (HPDT). It allows TCP/IP connections to the host through Cisco Mainframe Channel Connection (CMCC) adapters, using either the TCP/IP stack or the High Speed Access Services (HSAS) IP stack.

DistributedDirector

Cisco DistributedDirector provides dynamic, transparent, and scalable Internet traffic load distribution between multiple topologically dispersed servers. DistributedDirector is the only global Internet service scaling solution that utilizes Cisco Internetwork Operating System (Cisco IOS) software and leverages routing table information in the network infrastructure to make “network intelligent” load distribution decisions.

Using routing table intelligence in the network infrastructure, DistributedDirector transparently redirects end user service requests to the closest responsive server, as determined by client-to-server topological proximity and/or client-to-server response times, resulting in increased access performance seen by the end user and reduced transmission costs.

For Cisco IOS Release 12.0(3)T, the functionality of DistributedDirector from 11.1 IA is migrated to 12.0 T. Cisco DistributedDirector is only available as a special hardware/software bundle on the Cisco 2501, 2502, and the 4700-M platforms.

DLSw+ Enhanced Load Balancing

In a network with multiple capable paths, the DLSw+ Load Balancing Enhancements feature improves traffic load balancing between peers by distributing new circuits based on existing loads and the desired ratio.

For each capable peer (peers that have the lowest or equal cost specified), the DLSw+ Load Balancing feature calculates the difference between the desired and the actual ratio of circuits being used on a peer. It detects the path that is underloaded in comparison to the other capable peers and assigns new circuits to that path until the desired ratio is achieved.

DLSw+ Peer Clusters

The DLSw+ Peer Clusters feature reduces the explorer packet replication that typically occurs in a large DLSw+ Peer Group design, where there are multiple routers connected to the same LAN.

The DLSw+ Peer Clusters feature associates DLSw+ peers (that are connected to the same LAN) into logical groups. Once the multiple peers are defined in the same peer group cluster, the DLSw+ Border Peer recognizes that it does not have to forward explorers to more than one member within the same peer group cluster.

DLSw+ RSVP Bandwidth Reservation

The DLSw+ RSVP Bandwidth Reservation feature allows DLSw+ to reserve network bandwidth for the DLSw+ TCP connection between DLSw+ peers.

Although it has been possible in the past to reserve bandwidth for a particular existing DLSw+ peer connection through the RSVP CLI support in Cisco IOS software, the CLI required prior knowledge of the TCP ports for which the reservation was being made. Because DLSw+ uses one well-known port and one randomly assigned port, the reservation could not be made until after the peer connection was active.

The DLSw+ RSVP feature permits new DLSw+ peer connections to automatically request bandwidth reservations upon connection, thereby removing the need for user intervention after the peer is connected. This feature assures the reservation will survive a network or device failure and that the DLSw+ traffic carried over a TCP connection is not affected by congestion.

Fancy Queuing on Frame Relay for Cisco HDLC

In previous releases, when the **voice-encap** option was configured on Frame Relay or Cisco HDLC, all fancy queuing (such as weighted fair queuing, custom queuing, and priority queuing) on the interface was disabled, and queuing was handled on a first-come first-served (FCFS) basis. In this release, new enhancements have been made to support fancy queuing on Frame Relay and Cisco HDLC.

For Frame Relay, a new interface command, **frag-pre-queuing**, has been added that allows you to set the queuing to be performed after the data segmentation. The command is available for Frame Relay interfaces only. The syntax for this new command is the following:

frag-pre-queuing

no frag-pre-queuing

By default, this command is enabled, which allows only FCFS queuing at the interface level. If you enter **no frag-pre-queuing**, you can configure weighted fair queuing, custom queuing, or priority queuing at the interface level. Note that if you enter **no frag-pre-queuing**, you still must explicitly configure the fancy queuing type on the interface.

For HDLC encapsulation, the queuing now takes place after segmentation when the **voice-encap** option is entered. Weighted fair queuing, custom queuing, and priority queuing are now supported on an interface configured for Cisco HDLC.

Flow-based WRED

This feature provides a mechanism to penalize the flows that do not respond to Weighted Random Early Detection (WRED) drops. This feature is provided as an extension to the existing WRED functionality and can be turned on after WRED is turned on.

Flow-WRED ensures that no single flow can hog all the buffer resources at the output interface queue. With WRED alone, this can occur in the presence of traffic sources that do not back off during congestion. Flow-WRED maintains minimal information about the buffer occupancy per flow. Whenever a flow exceeds it's share of the output interface buffer resource the packets of the flow are penalized by increasing the probability of their drop (by WRED).

IP to ATM CoS with VC Bundle Management

This feature comprises the second phase of the IP to ATM Class of Service (CoS) feature made available with Release 11.1(22)CC. IP to ATM CoS with VC Bundle Management carries forward support for all commands and functionality provided by the first released phase of the feature, extending that support to operation on the Cisco 7200 series routers and enhancing it to include support for ATM VC bundle management.

ATM VC Bundle Management allows you to configure multiple permanent virtual circuits (PVCs) that have different quality of service (QoS) characteristics between any pair of ATM-connected routers. These VCs are grouped together in a bundle and are referred to as bundle members.

You define an ATM VC bundle and add VCs to it. Each VC of a bundle has its own ATM traffic class and ATM traffic parameters.You can apply attributes and characteristics to discrete VC bundle members or you can apply them collectively at the bundle level.

Using VC bundles, you can create differentiated service by flexibly distributing IP precedence levels over the different VC bundle members. You can map a single precedence level or a range of levels to each discrete VC in the bundle thereby enabling individual VCs in the bundle to carry packets marked with different precedence levels. You can use WRED to further differentiate service across traffic that has different IP precedence but that uses the same VC in a bundle.

ISDN BRI Voice over IP for Cisco 2600 and 3600 Series Routers

The Voice over IP feature enables the Cisco 3600 and Cisco 2600 series of modular routers to carry voice traffic simultaneously with data traffic over an IP network. Voice over IP (VoIP) is primarily a software feature, supporting both voice and fax calls. Support for the ISDN BRI signaling type allows a Cisco 3600 or Cisco 2600 series router to provide voice access connectivity to either an ISDN telephone network or to a digital interface on a PBX/key communications system. The voice or data also crosses an IP network to which the router connects. This allows branch offices and enterprises to route incoming public switched telephone network (PSTN) ISDN BRI calls over an IP network or send outgoing digital fax and voice calls via an IP network.

Large Scale Dialout

Large scale dialout eliminates the need to configure dialer maps on every network access server (NAS) for every destination. Instead, you create remote site profiles containing outgoing call attributes (telephone number, service type, maximum number of links, and so on) on an authentication, authorization, and accounting (AAA) server. The profile is downloaded by the NAS when packet traffic requires a call to be placed to a remote site. Large scale dialout also takes advantage of features previously only available for incoming calls, such as dialer and virtual profiles, Multichassis Multilink PPP (MMP) support, and the ability to use an AAA server to store dial out attributes. MMP allows NASes to be stacked together and appear as a single NAS chassis so that if one NAS fails, another NAS in the stack can accept calls. Additionally, large scale dialout addresses congestion management by seeking an uncongested, alternative NAS when the designated primary NAS experiences port congestion.

Multilink Inverse Multiplexer

The Multilink Point to Point Protocol (MLP) Inverse Multiplexer feature allows you to combine multiple T1/E1 lines in a Versatile Interface Processor (VIP) T1/E1 interface into a bundle that has the combined bandwidth of the multiple T1/E1 lines. This is done by using a VIP MLP link. You choose the number of bundles and the number of T1/E1 lines in each bundle. This allows you to increase the bandwidth of you network links beyond that of a single T1/E1 line without having to purchase a T3 line.

Multimedia Conference Manager

Use the Multimedia Conference Manager to enable your current internetwork to route bit-intensive data such as audio telephony, video and audio telephony, and data conferencing using existing telephone and ISDN links, without degrading the network's current level of service. The Multimedia Conference Manager feature provides H.323 application options previously unavailable. Using Multimedia Conference Manager, you can implement H.323-compliant applications on existing networks in an incremental fashion without upgrades. This feature also provides a rich list of networking capability, including:

- A means to implement Quality of Service (QoS), which is required for the successful deployment of H.323 applications.

- Inter-zone routing in the E.164 address space. When using H.323-ID format addresses, inter-zone routing is done through domain names.

The Multimedia Conference Manager feature provides network administration mechanisms to support H.323 applications without impacting the mission critical applications running on today's networks. Multimedia Conference Manager is implemented on Cisco IOS software. Multimedia Conference Manager provides the network administrator with these abilities:

- Identify H.323 traffic and apply appropriate policies
- Limit H.323 traffic on the local-area network (LAN) and wide-area network (WAN)
- Provide user accounting for records based on service utilization
- Insert QoS for the H.323 traffic generated by applications such as Voice over IP (VoIP), data conferencing, and video conferencing
- Implement security for H.323 communications

Multimedia Conference Manager has two principal functions: *gatekeeper* and *proxy.* This document describes the value of the Multimedia Conference Manager gatekeeper and proxy functions for end-to-end implementation of H.323-compliant multimedia applications. These functions are unique to Multimedia Conference Manager. Similar robust features are currently not available in other vendor solutions.

Gatekeeper subsystems provide:

- User authorization where authorization, authentication, and accounting (AAA) account holders are permitted to register and use the services of Multimedia Conference Manager
- Accounting using AAA call detail records
- Zone bandwidth management to limit the number of active sessions
- H.323 call routing
- Address resolution

Starting with Cisco IOS Releases 11.3(6)Q and 11.3(7)NA and later, you can configure Cisco gatekeepers to use the Cisco Hot Standby Routing Protocol (HSRP), so that when one gatekeeper fails, the standby gatekeeper assumes its role.

Proxy subsystems provide:

- H.323 traffic consolidation
- Tight bandwidth controls
- QoS mechanisms such as IP Precedence and RSVP
- Secure communication over extranets

NetFlow Policy Routing

IP policy routing now works with Cisco Express Forwarding (CEF), Distributed CEF (DCEF), NetFlow, and NetFlow with flow acceleration. IP policy routing was formerly supported only in fast-switching and process-switching. Now that policy routing is integrated into CEF, policy routing can be deployed on a wide scale and on high-speed interfaces.

Process MIB

The addition of the CISCO-PROCESS-MIB and changes to the CISCO-MEMORY-POOL-MIB allow the retrieval of additional CPU and memory statistics and their reporting by SNMP. The CISCO-PROCESS-MIB provides CPU 5-second, 1-minute, and 5-minute statistics. In addition, this MIB provides CPU utilization and memory allocation/deallocation statistics for each process on each CPU listed in the CISCO-PROCESS-MIB.

The CISCO-PROCESS-MIB is enabled when the first SNMP command is configured. The background statistics collection for VIP cards and the master CPU occurs even if the SNMP subsystem is not initialized.

Redundant Dial Shelf Controller

The Cisco AS5800 dial shelf can contain two Dial Shelf Controller (DSC) cards. The DSC card provides the following:

- Master clock for the dial shelf
- Fast Ethernet link to the router shelf
- Environmental monitoring of the feature boards
- Bootstrap images on start-up for the feature boards

With two DSC cards present, DSC redundancy provides for one DSC to act as a backup to the active one. If the active DSC fails, the backup provides the functionality. The primary aim is to increase system availability by preventing loss of service in the event of the failure of one of the DSCs.

This feature is automatically enabled when two DSC cards are installed. No configuration commands are required. (It is assumed that where the external DSC clocking port is configured, the clock signal fed into both DSCs is identical.) Console executive commands provided with this feature facilitate the use of the feature.

Response Time Reporter Enhancements

The Response Time Reporter (RTR) feature allows you to monitor network performance, network resources, and applications by measuring response times and availability. RTR statistics can be used to perform troubleshooting, problem notifications and pre-problem analysis. The RTR enhancements extend IP support, such as Type of Service, and allow you to measure various types of IP traffic, such as UDP, TCP, and HTTP.

RFC 1483 for Token Ring Networks

Cisco IOS Release 12.0(3)T supports RFC 1483 and enables the transfer of network interconnect traffic over ATM AAL5 layer, using LLC encapsulation. RFC 1483 defines an encapsulation type for transferring LAN data via ATM networks.

All LAN protocols that use the LLC format and run on Ethernet, Token Ring, or ATM networks are encapsulated in LLC data packets transported via ATM networks.

RSVP to ATM QoS Internetworking

The RSVP-ATM QoS networking feature provides support for Controlled Load Services using RSVP over an ATM core network. This feature requires the ability to signal for SVCs across the ATM cloud in response to RSVP reservation messages. To meet this requirement, RSVP over ATM supports mapping of RSVP sessions to ATM nonbroadcast multiaccess (NBMA) switched virtual circuits (SVCs).

RSVP over ATM allows you to configure an interface or subinterface to dynamically create SVCs in response to RSVP reservation requests. To ensure defined quality of service (QoS), these SVCs are established having QoS profiles consistent with the mapped RSVP flowspecs. To further support QoS, this feature allows you to configure the IP Precedence and ToS values to be used for packets that conform to or exceed QoS profiles. Moreover, it allows you to attach DWRED group definitions to the (PA-A3 ATM port adapter) interface to support per-VC DWRED drop policy, which ensures that if packets must be dropped, then best-effort packets are dropped first and not those that conform to the appropriate QoS determined by the RSVP's token bucket.

Service Provider Features for Voice over IP

The 12.0(3)T Cisco voice service provider features include enhancements made to the functionality and configuration of both the gateway and the Voice over IP (VoIP) gatekeeper. The architecture of these features provides the Quality of Service (QoS), stability, and functionality necessary for carrier class, real-time IP communications services.

This document contains a basic description of the H.323 VoIP gateway in addition to features required to implement the applications to run VoIP in a service provider environment. The features address the service provider needs to offer security, billing, scaling, and reliability.

The Cisco VoIP gateway is a high performance H.323-compliant gateway optimized for VoIP applications. Supporting up to two T1/E1 digital channels, it connects with existing telephones and fax machines through the Public Switched Telephone Network (PSTN), key systems, and PBXs, making the process of placing calls over the IP network transparent to users.

The gateway capability allows the Cisco VoIP gateway to function as an H.323 endpoint. Therefore, the gateway provides admission control, address lookup and translation, and accounting services.

The gatekeeper manages H.323 endpoints in a consistent manner, allowing them to register with the gatekeeper and to locate another gatekeeper. The gatekeeper provides logic variables for proxies or gateways in a call path to provide connectivity with the Public Switched Telephone Network (PSTN), to improve Quality Of Service (QoS), and to enforce security policies. Multiple gatekeepers may be configured to communicate with one another, either by integrating their addressing into Domain Naming System (DNS), or via Cisco I OS configuration options.

SLIP-PPP Banner and Banner Tokens

The SLIP-PPP Banner section of this feature enables you to configure the banner that is displayed when making a SLIP connection. This improves compatibility with non-Cisco SLIP dial-up software.

The Banner Tokens section of this feature introduces the use of tokens to all existing banner commands. Tokens allow you to display current information from the configuration, such as the router's hostname, IP address, encapsulation type, and MTU size.

SNMP v3

Simple Network Management Protocol version 3 (SNMPv3) addresses issues related to the large scale deployment of SNMP for configuration, accounting and fault management. Currently SNMP is predominantly used for monitoring and performance management. The primary goal of SNMPv3 is to define a secure version of the SNMP protocol. SNMPv3 also facilitates remote configuration of the SNMP entities which make remote administration of SNMP entities a much simpler task. SNMPv3 builds on top of SNMPv1 and SNMPv2 to provide a secure environment for the management of systems and networks.

SNMPv3 provides an identification strategy for SNMP devices to facilitate communication only between known SNMP strategy. Each SNMP device has an identifier called the SNMP EngineID which is a copy of SNMP. Each SNMP message contains an SNMP EngineID. SNMP communication is possible only if an SNMP entity knows the identity of its peer SNMP device.

SNMPv3 also contains a security model or security strategy that exists between an SNMP user and the SNMP group to which the user belongs. A security model may define the security policy within an administrative domain or a intranet. The SNMPv3 protocol consists of the specification for the User based Security Model (USM).

Definition of security goals where the goals of message authentication service includes the following protection strategies:

- **Modification of Information** or protection against some unauthorized SNMP entity altering in-transit SNMP messages generated on behalf of an authorized principal)
- **Masquerade** or protection against attempting management operations not authorized for some principal by assuming the identity of another principal that has the appropriate authorizations
- **Message Stream Modification** or protection against messages getting maliciously re-ordered, delayed or replayed in order to effect unauthorized management operations
- **Disclosure** or protection against eavesdropping on the exchanges between SNMP engines. Three different types of communication mechanisms are available for this protection strategy. They are:
  - communication without authentication and privacy (NoAuthNoPriv)
  - communication with authentication and without privacy (AuthNoPriv)
  - communication with authentication and privacy (AuthPriv)

SS7

Common Channel Signaling #7 (SS7) is a worldwide standard for switch to switch signaling in the public switched telephone network (PSTN). The Cisco SC2200 Signaling Controller provides centralized functions for adding Signaling System #7 (SS7) interfaces to remote access points of presence (POPs). The Cisco SC2200 signaling controller works together with Cisco access servers (AS5800, AS5300, and AS5200) to create a virtual switch, which functions from a signaling perspective as a terminating and originating end-office with SS7. Cisco access servers provide the interface from the circuit switched network to the data network. The protocol architecture for communication between Cisco's SC2200 signaling controller and access servers provides for reliable signaling over a IP infrastructure This feature provides the control protocol for Cisco access servers to support the Cisco SS7 dial access solution.

Tag Switch Controller (TSC)

The Tag Switch Controller (TSC) is a tag switch router (TSR) that controls the operation of a separate ATM switch. Together, the router and ATM switch function as a single ATM Tag Switching router (ATM-TSR). A Cisco 7200 or 7500 series router acts as the TSC and a Cisco BPX 8600 Service Node (8620 wide area switch or 8650 IP+ATM switch) or a partner's switch acts as the VSI-controlled ATM switch. The TSC controls the ATM switch using the Cisco Virtual Switch Interface (VSI), which runs over an ATM link connecting the two.

Token Ring MPOA

Token Ring Multiprotocol over ATM (MPOA) allows Token Ring hosts in an ATM network to communicate over alternate paths (called shortcuts) through the ATM network, which bypasses intermediate router hops that would otherwise be encountered in the default path.

Token Ring MPOA is an extension to LAN Emulation (LANE). Using the Next Hop Resolution Protocol (NHRP), and MPOA server (MPS) on the router, and MPO clients (MPCs) on the ATM edge devices, a direct virtual channel connection (VCC) between the ingress and egress edge devices is established. Token Ring MPOA allows Token Ring LANE clients to forward unicast IP packets between subnets to other Token Ring LANE clients through this shortcut VCC path on the ATM network.

Web Cache Communications Protocol Version 2 (WCCPv2)

The Web Cache Communications Protocol enables Cisco IOS routing platforms to transparently redirect content requests (for example, web requests) from clients to a locally connected Cisco Cache Engine (or Cache Cluster) instead of the intended origin server. When a Cache Engine receives such a request, it attempts to service it from its own local cache if the requested information is present. If not, the Cache Engine issues its own request to the originally requested origin server to get the required information. When the Cache Engine retrieves the requested information, it forwards it to the requesting client and caches it to fulfill future requests, thus maximizing download performance and significantly reducing WAN transmission costs.

WCCPv2 provides enhancements to WCCPv1, including:

- Multihome router support enables multiple co-located, WCCP-enabled routers to share a cache cluster.
- Improved security enables MD5 digital signature authentication (RFC 1321) to be used in Cache Engine/WCCP router communications.
- Redirection of non-port 80 traffic enables WCCP-enabled routers to transparently redirect traffic based on any TCP port (for example, FTP and NNTP traffic), in addition to HTTP traffic. Cache Engine-side support for non-port 80 traffic will be provided in the future.
- Content bypass support—When a Cache Engine rejects a request and sends it back to the WCCP-enabled router, the router knows not to redirect the request to the Cache Engine again.
- Flexible content distribution within a cache cluster—Various hashing parameters can be used to determine content distribution within a cache cluster.

X.25 Load Balancing

As the number of users accessing the same host has grown, competition for these application resources has become a problem. Internet service providers (ISPs) have had to increase the number of users they could support by increasing the number of X.25 lines to the host.

In order to support a large number of virtual circuits (VCs) to a particular destination, configuration of more than one serial interface to that destination was needed. When a serial interface is configured to support X.25, there is a fixed number of VCs available for use.

Using a facility called “hunt-group” (the method for X.25 load balancing), a switch is able to view a pool of X.25 lines going to the same host as one address and assign VCs on an “idle logical channel” basis. With this feature, X.25 calls can be load-balanced among all configured outgoing interfaces to fully use and balance all managed lines. The benefits include, the choice of two load-balancing distribution methods (rotary or vc-count) and improved performance of serial lines.

New Software Features in Release 12.0(2)T

There are no new features supported by the Cisco 2500 series in Cisco IOS Release 12.0(3)T.

New Software Features in Release 12.0(1)T

The following new software enhancements are supported by the Cisco 2500 series in Release 12.0(1)T.

RSM/TR-VLAN

The Token Ring VLAN support on the Route Switch Module (RSM) enables a Catalyst 5000 switch to provide the functionality of bridging and multi-protocol routing for Token Ring VLANs. The installation of an RSM in a Catalyst 5000 supplements the existing switching capabilities with the functionality of a standalone router that performs inter-VLAN routing and bridging. If the Token Ring RSM is associated with a VIP2 board, it provides direct external network connections through a variety of media using the standard port adapters on the VIP2 and offers functionality similar to a Cisco 7500 series router.

The RSM module can either route or bridge Token Ring packets, thereby functioning as a router or as a bridge. In Cisco IOS Release 12.0(1)T, both APPN and DLSW+ are supported on the RSM's Token Ring VLANs. RSRB, however, is not supported on the RSM.

IOS IEEE 802.1Q Support

Cisco IOS IEEE 802.1Q provides support for IEEE 802.1Q encapsulation for Virtual LANs (VLANs). Use this feature for VLANs consisting of IEEE 802.1Q compliant switches.

Mobile IP

Mobile IP provides users the freedom to roam beyond their home subnet while consistently maintaining their home IP address. This enables transparent routing of IP datagrams to mobile users during their movement, so that data sessions can be initiated to them while they roam; it also enables sessions to be maintained in spite of physical movement between points of attachment to the Internet or other networks. Cisco’s implementation of Mobile IP is fully compliant with the Internet Engineering Task Force’s (IETF’s) proposed standard defined in Request for Comments (RFC) 2002.

Easy IP Phase 2-DHCP Server

With the introduction of Easy IP Phase 2, Cisco IOS software also supports Intelligent DHCP Relay functionality. A DHCP Relay Agent is any host that forwards DHCP packets between clients and servers. A DHCP Relay Agent enables the client and server to reside on separate subnets. If the Cisco IOS DHCP server cannot satisfy a DHCP request from its own database, it can forward the DHCP request to one or more secondary DHCP servers defined by the network administrator using standard Cisco IOS ip helper-address functionality.

Smart-init (Mars FE2P)

The smart-init feature is an extension to the existing memory split program of the Cisco IOS software running on Cisco 3600 series routers. It computes iomem size by looking at the network modules installed in the system and uses this iomem for carrying out the memory split. Also, compatibility with older IOS configurations is maintained by retaining support for the **memory-size** configuration command. The user can disable smart-init and set iomem percentage to the required value by issuing the **memory-size** configuration command.

OSPF Packet Pacing

The former OSPF implementation for sending update packets needed to be more efficient. Some update packets were getting lost in cases where the link was slow, a neighbor could not receive the updates fast enough, or the router was out of buffer space. For example, packets might be dropped if either of these topologies existed:

- A fast router was connected to a slower router over a point-to-point link.
- During flooding, several neighbors dumped updates to a single router at the same time.

OSPF update packets are now automatically paced by a delay of 33 milliseconds. Pacing is also added between retransmissions to increase efficiency and minimize lost retransmissions.

OSPF update and retransmission packets are sent more efficiently. Also, you can display the LSAs waiting to be sent out an interface.

Time-Based Access Lists

It is now possible to implement access lists based on the time of day. To do so, you create a time range that defines specific times of the day and week. The time range is identified by a name, and then referenced by a function, so that those time restrictions are imposed on the function itself.

Currently, IP and IPX extended access lists are the only functions that can use time ranges. The time range allows the network administrator to define when the permit or deny statements in the access list are in effect. Prior to this feature, access list statements were always in effect once they were applied. Both named or numbered access lists can reference a time range.

RIP Enhancements

Triggered extensions to IP RIP increase efficiency of RIP on point-to-point, serial interfaces.

Routers are used on connection-oriented networks to allow potential connectivity to many remote destinations. Circuits on the WAN are established on demand and are relinquished when the traffic subsides. Depending on the application, the connection between any two sites for user data could be short and relatively infrequent.

There were two problems using RIP to connect to a WAN:

- Periodic broadcasting by RIP generally prevented WAN circuits form being closed.
- Even on fixed, point-to-point links, the overhead of periodic RIP transmissions could seriously interrupt normal data transfer because of the quantity of information that hits the line every 30 seconds.

To overcome these limitations, triggered extensions to RIP cause RIP to send information on the WAN only when there has been an update to the routing database. Periodic update packets are suppressed over the interface on which this feature is enabled.

Cisco IOS Firewall Feature Set Platform Support

The Cisco IOS Firewall feature set is now available on 2600 and 3600 series products.

The Cisco IOS Firewall feature set extends the security technology currently available in Cisco IOS software to provide firewall specific capabilities:

- Context-based Access Control (CBAC)
- Java blocking

- Denial-of-service detection and prevention
- Real-time alerts and audit trails

The Cisco IOS Firewall feature set adds advanced filtering capabilities to existing security functionality in Cisco routers. Some existing Cisco IOS security features include packet filtering via access control lists (ACLs), Network Address Translation (NAT), network-layer encryption, and TACACS+ authentication.

ISDN MIB RFC2127

The new Integrated Services Digital Network (ISDN) Management Information Base (MIB) RFC2127 has been designed to provide useful information in accordance with the IETF's new standard for the management of ISDN interfaces. It controls all aspects of ISDN interfaces. RFC2127 provides information on the physical Basic Rate Interfaces (BRIs), control and statistical information for B (bearer) and D (signaling) channels, terminal endpoints, and directory numbers.

IOS STP Enhancements

IOS Spanning Tree Protocol enhancements broaden the original IOS STP implementation with increased port identification capability, improved path cost determination, and support for a new VLAN bridge spanning-tree protocol.

Layer Two Tunneling Protocol (L2TP)

Layer Two Tunneling Protocol (L2TP) is an emerging Internet Engineering Task Force (IETF) standard that combines the best features of two existing tunneling protocols: Cisco's Layer Two Forwarding (L2F) and Microsoft's Point-to-Point Tunneling Protocol (PPTP). L2TP is an extension to the Point-to-Point Protocol (PPP), which is an important component for Access Virtual Private Networks (VPNs). Access VPNs allow mobile users to connect to their corporate intranets or extranets, thus improving flexibility and reducing costs.

Traditional dial-up networking services only supported registered IP address, which limited the types of applications that could be implemented over Virtual Private Networks (VPNs). L2TP supports multiple protocols and unregistered and privately administered IP addresses over the Internet. This allows the existing access infrastructure, such as the Internet, modems, access servers, and ISDN terminal adaptors (TAs), to be used.

L2TP can be initiated wherever PPTP or L2F is currently deployed and can be operated as a client initiated tunnel, such as PPTP, or a network access server (NAS) initiated tunnel, such as L2F.

PPP Over Frame Relay

The PPP over Frame Relay feature allows a router to establish end-to-end Point-to-Point Protocol (PPP) sessions over Frame Relay. IP datagrams are transported over the PPP link using RFC 1973 compliant Frame Relay framing. This feature is useful for remote users running PPP to access their Frame Relay corporate networks.

PPP over Frame Relay provides the following benefits:

- Allows end-to-end PPP sessions over Frame Relay.
- Supports the 90i IDSL Channel Unit that supports both Frame Relay and Point-to-Point Protocol (PPP) on an ISDN DSL.

IETF Compliant PPP over ATM Scalability

Point-to-Point Protocol (PPP) over Asynchronous Transfer Mode (ATM) is now available on an ATM CES port adapter in a Cisco 7200-series router.

In previous releases of PPP over ATM, you configured permanent virtual circuits (PVCs) for PPP over ATM on point-to-point subinterfaces. In this release, each PPP over ATM connection no longer requires two interfaces, a virtual access interface and ATM subinterface. Instead, you can configure multiple PVCs for PPP over ATM on multipoint subinterfaces, thereby providing a significant increase in the number of PPP over ATM sessions per router. Also in this release, PPP over ATM is enhanced to support virtual circuit (VC) multiplexed encapsulation and complies with the Internet Engineering Task Force (IETF) draft on multiplexed encapsulation titled PPP over AAL5. The previous version of PPP over ATM supported only the Frame Forwarding data encapsulation (aal5ciscoppp).

Note The IETF PPP over ATM feature does not currently support LLC encapsulated PPP over ATM Adaptation Layer 5 (AAL5).

This release of the PPP over ATM feature provides support for IETF-compliant PPP over ATM and significantly increases the maximum number of PPP over ATM sessions running on a router. The maximum number of PPP over ATM sessions supported on a platform depends on available system resources such as memory and CPU speed.

Data Compression Advanced Interface Module

This document describes how to configure, verify, and troubleshoot the Data Compression features of the Advanced Interface Module (AIM) on Cisco 2600 Series Routers. The Data Compression AIM provides hardware-based compression and decompression of packet data transmitted and received on the serial network interfaces of Cisco 2600 Series Routers without occupying the Port Module Slot, that might otherwise be used for additional customer network ports. Supported are the industry standard LZS and MPPC compression algorithms. The Data Compression AIM requires Cisco IOS Release 12.0(1)T, or later 12.0 T releases.

ATM PVC Trap Support

The ATM PVC Trap Support feature provides Simple Network Management Protocol (SNMP) notification for permanent virtual circuit (PVC) failures, and it provides SNMP access to PVC status tables.

Normally, a management station is not notified when an Asynchronous Transfer Mode (ATM) PVC goes down. The ATM PVC Trap Support feature enables an agent to send the required PVC traps for this notification. It also provides support for these PVC status tables: atmCurrentlyFailingPVclTable and atmInterfaceExtTable.

Important Notes

The following sections contain important notes about Cisco IOS Release 12.0 that can apply to the Cisco 2500 series.

Cisco IOS Syslog Failure

Certain versions of Cisco IOS software may fail or hang when they receive invalid User Datagram Protocol (UDP) packets sent to their syslog ports (port 514). At least one commonly used Internet scanning tool generates packets that cause such problems. This fact has been published on public Internet mailing lists, which are widely read both by security professionals and by security crackers. This information should be considered in the public domain.

Attackers can cause Cisco IOS devices to repeatedly fail and reload, resulting in a completely disabled Cisco IOS device that needs to be reconfigured by its administrator. Some Cisco IOS devices have been observed to hang instead of failing when attacked. These devices do not recover until they are manually restarted by reset or power cycling. An administrator must personally visit an attacked, hung device to restart it, even if the attacker is no longer actively sending any traffic. Some devices have failed without providing stack traces; some devices may indicate that they were "restarted by power-on," even when that is not the case.

Assume that any potential attacker is likely to know that existence of this problem and the ways to exploit it. An attacker can use tools available to the public on the Internet and does not need to write any software to exploit the vulnerability. Minimal skill is required and no special equipment is required.

Despite Cisco specifically inviting such reports, Cisco has received no actual reports of malicious exploitation of this problem.

This vulnerability notice was posted on Cisco's World Wide Web site:

http://www.cisco.com/warp/public/770/iossyslog-pub.shtml

This information was also sent to the following e-mail and USENET news recipients:

- cust-security-announce@cisco.com
- bugtraq@netspace.org
- first-teams@first.org (includes CERT/CC)
- first-info@first.org
- cisco@spot.colorado.edu
- comp.dcom.sys.cisco
- nanog@merit.edu

Affected Devices and Software Versions

Vulnerable devices and software versions are specified in Table 7, Affected and Repaired Software Versions. Affected versions include Releases 11.3 AA, 11.3 DB, and all 12.0 versions (including 12.0 mainline, 12.0 S, 12.0 T, and any other regular released version whose number starts with 12.0), up to the repaired releases listed in Table 7. Cisco is correcting the problem in certain special releases and will correct it in future maintenance and interim releases. See Table 7, Affected and Repaired Software Versions for details. Cisco intends to provide fixes for all affected IOS variants.

No particular configuration is needed to make a Cisco IOS device vulnerable. It is possible to filter out attack traffic by using access lists. See the "Workarounds" section on page 31 for techniques. However, except at Internet firewalls, the appropriate filters are not common in customer configurations. Carefully evaluate your configuration before assuming that any filtering you have protects you against this attack.

The most commonly used or asked-about products are listed below. If you are unsure whether your device is running Cisco IOS software, log in to the device and issue the **show version** command. Cisco IOS software will identify itself simply as "IOS" or "Internetwork Operating System Software". Other Cisco devices will not have the **show version** command, or they will identify themselves differently in their output. The most common Cisco devices that run Cisco IOS software include the following:

- Cisco routers in the AGS/MGS/CGS/AGS+, IGS, RSM, 800, uBR900, 1000, 2500, 2600, 3000, 3600, 3800, 4000, 4500, 4700, AS5200, AS5300, AS5800, 6400, 7000, 7200 (including the uBR7200), 7500, and 12000 series
- Most recent versions of the LS1010 ATM switch
- Some versions of the Catalyst 2900XL LAN switch
- Cisco DistributedDirector

Affected software versions, which are relatively new, are not necessarily available on every device listed above. If you are not running Cisco IOS software, you are not affected by this problem.

The following Cisco devices are *not* affected:

- 700 dialup routers (750, 760, and 770 series)
- Catalyst 1900, 2800, 2900, 3000, and 5000 LAN switches are not affected, except for some versions of the Catalyst 2900XL. However, optional router modules running Cisco IOS software in switch backplanes, such as the RSM module for the Catalyst 5000 and 5500, are affected.
- WAN switching products in the IGX and BPX lines
- MGX (formerly known as the AXIS shelf)
- Host-based software
- Cisco PIX Firewall
- Cisco LocalDirector
- Cisco Cache Engine

This vulnerability has been assigned Cisco bug ID CSCdk77426.

Solution

Cisco offers free software updates to correct this vulnerability for all affected customers—regardless of their contract status. However, because this vulnerability information has been disseminated by third parties, Cisco has released this notice before updates are available for all software versions. Table 7 gives Cisco's projected fix dates.

Make sure your hardware has adequate RAM to support the new software before installing it. The amount of RAM is seldom a problem when you upgrade within a major release (say, from 11.2[11]P to 11.2[17]P), but it is often a factor when you upgrade between major releases (say, from 11.2 P to 11.3 T).

Because fixes will be available for all affected releases, this vulnerability will rarely, if ever, require an upgrade to a new major release. Cisco recommends very careful planning for any upgrade between major releases. Make certain no known bugs will prevent the new software from working properly in your environment.

Further upgrade planning assistance is available on Cisco's World Wide Web site at:

http://www.cisco.com

If you have service contracts you can obtain new software through your regular update channels (generally through Cisco's World Wide Web site). You can upgrade to any software release, but you must remain within the boundaries of the feature sets you have purchased.

If you do not have service contracts, you can upgrade to obtain only the bug fixes; free upgrades are restricted to the minimum upgrade required to resolve the defects. In general, you will be restricted to upgrading within a single row of Table 7, except when no upgrade within the same row is available in a timely manner. Obtain updates by contacting one of the following Cisco Technical Assistance Centers (TACs):

- +1 800 553 2447 (toll-free from within North America)
- +1 408 526 7209 (toll call from anywhere in the world)
- tac@cisco.com

Give the URL of this notice (http://www.cisco.com/warp/public/770/iossyslog-pub.shtml) as evidence for a free update. Non-contract customers must request free updates through the TAC. Please do not contact either "psirt@cisco.com" or "security-alert@cisco.com" for software updates.

Workarounds

You can work around this vulnerability by preventing any affected Cisco IOS device from receiving or processing UDP datagrams addressed to its port 514. This can be done either by using packet filtering on surrounding devices, or by using input access list filtering on the affected IOS device itself.

If you use an input access list, apply that list to all interfaces to which attackers may be able to send datagrams. Interfaces include not only physical LAN and WAN interfaces but also virtual subinterfaces of those physical interfaces, as well as virtual interfaces and interface templates corresponding to GRE, L2TP, L2F, and other tunneling protocols.

The input access list must block traffic destined for UDP port 514 at any of the Cisco IOS device's own IP addresses, as well as at any broadcast or multicast addresses on which the Cisco IOS device may be listening. Be sure to block both old-style "all-zeros" broadcasts and new-style "all-ones" broadcasts. It is not necessary to block traffic being forwarded to other hosts—only traffic actually addressed to the Cisco IOS device is of interest.

No single input access list works in all configurations. Know the effect of your access list in your specific configuration before activating it.

The following example shows a possible access list for a three-interface router, along with the configuration commands needed to apply the list. The example assumes input filtering is not needed, other than as a workaround for this problem:

```
! Deny all multicasts, and all unspecified-net broadcasts, to port 514
access-list 101 deny udp any 224.0.0.0 31.255.255.255 eq 514
! Deny old-style unspecified-net broadcasts
access-list 101 deny udp any host 0.0.0.0 eq 514
! Deny network-specific broadcasts. This example assumes that all of
! the local interfaces are on the class B network 172.16.0.0, subnetted
! everywhere with mask 255.255.255.0. This will differ from network
! to network. Note that we block both new-style and old-style broadcasts.
access-list 101 deny udp any 172.16.0.255 0.0.255.0 eq 514
access-list 101 deny udp any 172.16.0.0   0.0.255.0 eq 514
! Deny packets sent to the addresses of our own network interfaces.
access-list 101 deny udp any host 172.16.1.1 eq 514
access-list 101 deny udp any host 172.16.2.1 eq 514
access-list 101 deny udp any host 172.16.3.3 eq 514
! Permit all other traffic (default would be to deny)
access-list 101 permit ip any any

! Apply the access list to the input side of each interface
interface ethernet 0
ip address 172.16.1.1 255.255.255.0
ip access-group 101 in

interface ethernet 2
ip address 172.16.2.1 255.255.255.0
ip access-group 101 in

interface ethernet 3
ip address 172.16.3.3 255.255.255.0
ip access-group 101 in
```

Listing all possible addresses—especially all possible broadcast addresses—to which attack packets may be sent is complicated. If you do not need to forward any legitimate syslog traffic received on an interface, you can block all syslog traffic arriving on that interface. Remember that blocking will affect traffic routed through the Cisco IOS device as well as traffic destined to the device; if the IOS device is expected to forward syslog packets, you will have to do the detailed filtering. Because input access lists impact system performance, install them with caution—especially on systems running very near their capacity.

Software Versions and Fixes

Many Cisco software images have been or will be specially reissued to correct this vulnerability. For example, regular released Cisco IOS version 12.0(2) is vulnerable, as are interim versions 12.0(2.1) through 12.0(2.3). The first fixed interim version of Release12.0 mainline software is Release12.0(2.4). However, a special release, 12.0(2a), contains only the fix for this vulnerability and does not include any other bug fixes from later 12.0 interim releases.

If you are running Release 12.0(2) and want to fix this problem without risking possible instability presented by installing the 12.0(2.4) interim release, you can upgrade to Release 12.0(2a). Release 12.0(2a) is a “code branch” from the Release 12.0(2) base, which will merge back into the Release 12.0 mainline at Release 12.0(2.4).

Special releases, like 12.0(2a), are one-time, spot fixes, and they will not be maintained. Thus, the upgrade path from Release 12.0(2a) is to Release 12.0(3).

Table 7 specifies information about affected and repaired software versions.

Note All dates within this table are subject to change.

Table 7 Affected and Repaired Software Versions

Cisco IOS Major Release	Description	Special Fix[1]	First Fixed Interim Release[2]	Fixed Maintenance Release[3]
Unaffected Releases				
11.2 and earlier releases—all variants	Unaffected early releases (no syslog server)	Unaffected	Unaffected	Unaffected
11.3, 11.3 T, 11.3 DA, 11.3 MA, 11.3 NA, 11.3 WA, 11.3(2)XA	11.3 releases without syslog servers	Unaffected	Unaffected	Unaffected
Releases Based on 11.3				
11.3 AA	11.3 early deployment for AS58xx	11.3(7)AA2, 8-JAN-1999[4]	11.3(7.2)AA	11.3(8)AA, 15-FEB-1999
11.3 DB	11.3 for Cisco NRP routing blade in Cisco 6400 xDSL DSLAM			11.3(7)DB2, 18-JAN-1999
Releases Based on 12.0				
12.0	12.0 Mainline	12.0(2a), 8-JAN-1999	12.0(2.4)	12.0(3), 1-FEB-1999
12.0 T	12.0 new technology early deployment	12.0(2a)T1, 11-JAN-1999	12.0(2.4)T	12.0(3)T, 15-FEB-1999
12.0 S	ISP support; 7200, RSP, GSR		12.0(2.3)S, 27-DEC-1998	12.0(2)S[5], 18-JAN-1999
12.0 DB	12.0 for Cisco 6400 universal access concentrator node switch processor (lab use)			12.0(2)DB, 18-JAN-1999
12.0(1)W	12.0 for Catalyst 8500 and LS1010	12.0(1)W5(5a) and 12.0(1a)W5(5b) (LS1010 platform only)	12.0(1)W5(5.15)	12.0(1)W5(6) (platform support for Catalyst 8540M will be in 12.0(1)W5(7))
12.0(0.6)W5	One-time early deployment for CH-OC-12 module in Catalyst 8500 series switches	Unaffected; one-time release	Unaffected	Unaffected; To upgrade use 12.0(1)W5 releases.
12.0(1)XA3	Short-life release; merged to 12/0T at 12.0(2)T	Obsolete	Merged	Upgrade to 12.0(2a)T1 or to 12.0(3)T.
12.0(1)XB	Short-life release for Cisco 800 series; merged to 12.0 T and 12.0 (3)T	12.0(1)XB1	Merged	Upgrade to 12.0(3)T.
12.0(2)XC	Short-life release for new features in Cisco 2600, Cisco 3600, uBR7200, uBR900 series; merged to 12.0 T at 12.0(3)T	12.0(2)XC1, 7-JAN-1999	Merged	Upgrade to 12.0(3)T

Table 7 Affected and Repaired Software Versions (continued)

Cisco IOS Major Release	Description	Special Fix[1]	First Fixed Interim Release[2]	Fixed Maintenance Release[3]
12.0(2)XD	Short-life release for ISDN voice features; merged to 12.0 T at 12.0(3)T	12.0(2)XD1, 18-JAN-1999	Merged	Upgrade to 12.0(3)T
12.0(1)XE	Short-life release	12.0(2)XE, 18-JAN-1999	Merged	Upgrade to 12.0(3)T

1 A special fix is a one-time release that provides the most stable immediate upgrade path.
2 Interim releases are tested less rigorously than regular maintenance releases; interim releases can contain serious bugs.
3 Fixed maintenance releases are on a long-term upgrade path. Other long-term upgrade paths also exist.
4 All dates in this table are estimates and are subject to change.
5 This entry is not a misprint. The 12.0(2.3)S interim release is available before the 12.0(2)S regular release.

Deprecated MIBs

Old Cisco Management Information Bases (MIBs) will be replaced in a future release. OLD-CISCO-* MIBs are currently being migrated into more scalable MIBs—without affecting existing Cisco IOS products or NMS applications. You can update from deprecated MIBs to the replacement MIBs as shown inTable 8.

Table 8 Deprecated and Replacement MIBs

Deprecated MIB	Replacement
OLD-CISCO-APPLETALK-MIB	RFC1243-MIB
OLD-CISCO-CHASSIS-MIB	ENTITY-MIB
OLD-CISCO-CPUK-MIB	In development
OLD-CISCO-DECNET-MIB	
OLD-CISCO-ENV-MIB	CISCO-ENVMON-MIB
OLD-CISCO-FLASH-MIB	CISCO-FLASH-MIB
OLD-CISCO-INTERFACES-MIB	IF-MIB CISCO-QUEUE-MIB
OLD-CISCO-IP-MIB	
OLD-CISCO-MEMORY-MIB	CISCO-MEMORY-POOL-MIB
OLD-CISCO-NOVELL-MIB	NOVELL-IPX-MIB
OLD-CISCO-SYS-MIB	(Compilation of other OLD* MIBs)
OLD-CISCO-SYSTEM-MIB	CISCO-CONFIG-COPY-MIB
OLD-CISCO-TCP-MIB	CISCO-TCP-MIB
OLD-CISCO-TS-MIB	
OLD-CISCO-VINES-MIB	CISCO-VINES-MIB
OLD-CISCO-XNS-MIB	

Caveats

Caveats describe unexpected behavior or defects in Cisco IOS software releases. For information on caveats in Cisco IOS Release 12.0 T, refer to the *Caveats for Cisco IOS Release 12.0 T* document.

All caveats in Release 12.0 are also in Release 12.0 T.

For information on caveats in Cisco IOS Release 12.0, refer to the *Caveats for Cisco IOS Release 12.0* document, which lists severity 1 and 2 caveats, and is located on CCO and the Documentation CD-ROM. Severity 1 caveats are the most serious caveats; severity 2 caveats are less serious.

Note If you have an account with CCO, you can use Bug Navigator II to find caveats of any severity for any release. From CCO, log in and click on this path: **Service & Support**: **Online Technical Support**: **Software Bug Toolkit**. You can also find Bug Navigator II at http://www.cisco.com/support/bugtools.

Related Documentation

The following sections describe the documentation available for the Cisco 2500 series. Typically, these documents consist of hardware and software installation guides, Cisco IOS configuration and command references, system error messages, feature modules, and other documents.

Documentation is available as printed manuals or electronic documents, except for feature modules, which are available online on CCO and the Documentation CD-ROM.

Use these release notes with the documents listed in the following sections:

- Release-Specific Documents, page 35
- Platform-Specific Documents, page 36
- Feature Modules, page 36
- Cisco IOS Software Documentation Set, page 37

Release-Specific Documents

The following documents are specific to Release 12.0. They are located on CCO and the Documentation CD-ROM:

- *Release Notes for Cisco IOS Release 12.0*

  To reach the *Cross-Platform Release Notes for Cisco IOS Release 12.0* from CCO, click on this path:

  Service & Support: **Documentation Home Page**: **Cisco IOS Software Configuration**: **Cisco IOS Release 12.0**: **Release Notes**: **Cross-Platform Release Notes**

  To reach the *Cross-Platform Release Notes for Cisco IOS Release 12.0* on the Documentation CD-ROM, click on this path:

  Cisco Product Documentation: Cisco IOS Software Configuration: **Cisco IOS Release 12.0**: **Release Notes**: **Cross-Platform Release Notes**

- Product bulletins, field notices, and other release-specific documents

  To reach these documents from CCO, click on this path:

  Service & Support: **Technical Documents**

- *Caveats for Cisco IOS Release 12.0 T*

  As a supplement to the caveats listed in the "Caveats" section on page 35 section in these release notes, see the *Caveats for Cisco IOS Release 12.0* and *Caveats for Cisco IOS Release 12.0 T* documents, which contains caveats applicable to all platforms for all maintenance releases of Release 12.0.

  To reach the caveats document from CCO, click on this path:

  Service & Support: Documentation Home Page: **Cisco IOS Software Configuration**: **Cisco IOS Release 12.0**: **Caveats**

  To reach the caveats document on the Documentation CD-ROM, click on this path:

  Cisco Product Documentation: Cisco IOS Software Configuration: **Cisco IOS Release 12.0**: **Caveats**

Note If you have an account with CCO, you can use Bug Navigator II to find caveats of any severity for any release. From CCO, log in and click on this path: **Service & Support**: **Online Technical Support**: **Software Bug Toolkit**. You can also find Bug Navigator II at http://www.cisco.com/support/bugtools.

Platform-Specific Documents

These documents are available for the Cisco 2500 series on CCO and the Documentation CD-ROM.

- *Cisco 2524 and Cisco 2525 Public Network Certification*
- *Installing WAN Modules in the Cisco 2524 and Cisco 2525 Routers*
- *Cisco 2524 and Cisco 2525 Router User Guide*
- *Redundant Power Systems*

To reach Cisco 2500 series documentation from CCO, click on this path:

Service & Support: Documentation Home Page: Access Servers and Access Routers: Modular Access Routers: Cisco 2500 Series Routers

To reach Cisco 2500 series documentation on the Documentation CD-ROM, click on this path:

Cisco Product Documentation: Access Servers and Access Routers: Modular Access Routers: Cisco 2500 Series Routers

Feature Modules

Feature modules describe new features supported by Release 12.0 T and are updates to the Cisco IOS documentation set. A feature module consists of a brief overview of the feature, benefits, configuration tasks, and a command reference. As updates, the feature modules are available online only. Feature module information is incorporated in the next printing of the Cisco IOS documentation set.

To reach the feature modules from CCO, click on this path:

Service & Support: Documentation Home Page: Cisco IOS Software Configuration: **Cisco IOS Release 12.0**: **New Feature Documentation**

To reach the feature modules on the Documentation CD-ROM, click on this path:

Cisco Product Documentation: Cisco IOS Software Configuration: **Cisco IOS Release 12.0**: **New Feature Documentation**

Cisco IOS Software Documentation Set

The Cisco IOS software documentation set consists of the Cisco IOS configuration guides, Cisco IOS command references, and several other supporting documents. These documents are shipped with your order in electronic form on the Documentation CD-ROM—unless you specifically ordered the printed versions.

Documentation Modules

Each module in the Cisco IOS documentation set consists of two books: a configuration guide and a corresponding command reference. Chapters in a configuration guide describe protocols, configuration tasks and Cisco IOS software functionality, and they contain comprehensive configuration examples. Chapters in a command reference provide complete command syntax information. Use each configuration guide with its corresponding command reference.

On CCO and the Documentation CD-ROM, two master hot-linked documents provide information for the Cisco IOS software documentation set: configuration guides and command references.

To reach these documents from CCO, click on this path:

Service & Support: Documentation Home Page: Cisco IOS Software Configuration: Cisco IOS Release 12.0: Configuration Guides and Command References

To reach these documents on the Documentation CD-ROM, click on this path:

Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 12.0: Configuration Guides and Command References

Release 12.0 Documentation Set

Table 9 describes the contents of the Cisco IOS Release 12.0 software documentation set, which is available in electronic form and in printed form upon request.

Note You can find the most current Cisco IOS documentation on CCO and the Documentation CD-ROM. These electronic documents may contain updates and modifications made after the hard-copy documents were printed.

To reach the Cisco IOS documentation set from CCO, click on this path:

Service & Support: Documentation Home Page: Cisco IOS Software Configuration: Cisco IOS Release 12.0

To reach the Cisco IOS documentation set on the Documentation CD-ROM, click on this path:

Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 12.0

Table 9 Cisco IOS Software Release 12.0 Documentation Set

Books	Chapter Topics
• *Configuration Fundamentals Configuration Guide* • *Configuration Fundamentals Command Reference*	Configuration Fundamentals Overview Cisco IOS User Interfaces File Management System Management
• *Bridging and IBM Networking Configuration Guide* • *Bridging and IBM Networking Command Reference*	Transparent Bridging Source-Route Bridging Token Ring Inter-Switch Link Remote Source-Route Bridging DLSw+ STUN and BSTUN LLC2 and SDLC IBM Network Media Translation DSPU and SNA Service Point SNA Frame Relay Access Support APPN Cisco Database Connection NCIA Client/Server Topologies Cisco Mainframe Channel Connection Airline Product Set
• *Dial Solutions Configuration Guide* • *Dial Solutions Command Reference*	Dial-In Port Setup Dial-In Terminal Services Dial-on-Demand Routing (DDR) Dial Backup Dial-Out Modem Pooling Large-Scale Dial Solutions Cost-Control Solutions ISDN X.25 over ISDN VPDN Dial Business Solutions and Examples
• *Cisco IOS Interface Configuration Guide* • *Cisco IOS Interface Command Reference*	Interface Configuration Overview
• *Network Protocols Configuration Guide, Part 1* • *Network Protocols Command Reference, Part 1*	IP Addressing IP Services IP Routing Protocols
• *Network Protocols Configuration Guide, Part 2* • *Network Protocols Command Reference, Part 2*	AppleTalk Novell IPX
• *Network Protocols Configuration Guide, Part 3* • *Network Protocols Command Reference, Part 3*	Apollo Domain Banyan VINES DECnet ISO CLNS XNS
• *Security Configuration Guide* • *Security Command Reference*	AAA Security Services Security Server Protocols Traffic Filtering and Firewalls IP Security and Encryption Passwords and Privileges Neighbor Router Authentication IP Security Options

Table 9 Cisco IOS Software Release 12.0 Documentation Set (continued)

Books	Chapter Topics
• *Cisco IOS Switching Services Configuration Guide* • *Cisco IOS Switching Services Command Reference*	Switching Paths for IP Networks Virtual LAN (VLAN) Switching and Routing
• *Wide-Area Networking Configuration Guide* • *Wide-Area Networking Command Reference*	ATM Frame Relay SMDS X.25 and LAPB
• *Voice, Video, and Home Applications Configuration Guide* • *Voice, Video, and Home Applications Command Reference*	Voice over IP Voice over Frame Relay Voice over ATM Voice over HDLC Video Support Universal Broadband Features
• *Quality of Service Solutions Configuration Guide* • *Quality of Service Solutions Command Reference*	Classification Scheduling Packet Drop Traffic Shaping ATM QoS SNA QoS Line Protocols
• *Cisco IOS Software Command Summary* • *Dial Solutions Quick Configuration Guide* • *System Error Messages* • *Debug Command Reference*	

Note The *Cisco Management Information Base (MIB) User Quick Reference* publication is no longer published. For the latest list of MIBs supported by Cisco, see *Cisco Network Management Toolkit* on Cisco Connection Online. From CCO, click on the following path: **Service & Support: Software Center: Network Mgmt Products: Cisco Network Management Toolkit: Cisco MIB**.

Service and Support

For service and support for a product purchased from a reseller, contact the reseller. Resellers offer a wide variety of Cisco service and support programs that are described in the "Service and Support" section of the *Cisco Information Packet* shipped with your product.

Note If you purchased your product from a reseller, you can access CCO as a guest. CCO is Cisco Systems' primary real-time support channel. Your reseller offers programs that include direct access to CCO services.

For service and support for a product purchased directly from Cisco, use CCO.

Software Configuration Tips on the Cisco Technical Assistance Center Home Page

If you have a CCO login account, you can access the following URL, which contains links and helpful tips on configuring your Cisco products:

http://www.cisco.com/kobayashi/serv_tips.shtml

This URL is subject to change without notice. If it changes, point your Web browser to CCO and click on this path: **Products & Technologies: Products: Technical Tips.**

The following sections are provided from the Technical Tips page:

- Access Dial Cookbook—Contains common configurations or recipes for configuring various access routes and dial technologies.
- Field Notices—Designed to notify you of any critical issues regarding Cisco products. These notices include problem descriptions, safety or security issues, and hardware defects.
- Frequently Asked Questions—Collection of the most frequently asked technical questions about Cisco hardware and software.
- Hardware—Technical Tips related to specific hardware platforms.
- Hot Tips—Popular tips and hints gathered from the Cisco Technical Assistance Center (TAC). Most of these documents are available from the TAC Fax-on-demand service. To reach Fax-on-demand and receive documents at your fax machine from the United States, call 888-50-CISCO (888-502-4726). From other areas, call 650-596-4408.
- Internetworking Features—Tips on using and deploying Cisco IOS software features and services.
- Sample Configurations—Actual configuration examples that are complete with topology and annotations.
- Software Products—Cisco IOS Software Bulletins, Cisco TCP/IP Suite 100, General Cisco IOS, Internet/Intranet Applications and Software, Network Management, Network Protection Software Tips, and WAN Switching Products and Software.
- Special Collections—Other helpful documents, including Case Studies, References & Request for Comments (RFCs), and Security Advisories.

Cisco Connection Online

Cisco Connection Online (CCO) is Cisco Systems' primary, real-time support channel. Maintenance customers and partners can self-register on CCO to obtain additional information and services.

Available 24 hours a day, 7 days a week, CCO provides a wealth of standard and value-added services to Cisco's customers and business partners. CCO services include product information, product documentation, software updates, release notes, technical tips, the Bug Navigator, configuration notes, brochures, descriptions of service offerings, and download access to public and authorized files.

CCO serves a wide variety of users through two interfaces that are updated and enhanced simultaneously: a character-based version and a multimedia version that resides on the World Wide Web (WWW). The character-based CCO supports Zmodem, Kermit, Xmodem, FTP, and Internet e-mail, and it is excellent for quick access to information over lower bandwidths. The WWW version of CCO provides richly formatted documents with photographs, figures, graphics, and video, as well as hyperlinks to related information.

You can reach CCO in the following ways:

- WWW: http://www.cisco.com
- WWW: http://www-europe.cisco.com
- WWW: http://www-china.cisco.com
- Telnet: cco.cisco.com
- Modem: From North America, 408 526-8070; from Europe, 33 1 64 46 40 82. Use the following terminal settings: VT100 emulation; databits: 8; parity: none; stop bits: 1; and connection rates up to 28.8 kbps.

For a copy of CCO's Frequently Asked Questions (FAQ), contact cco-help@cisco.com. For additional information, contact cco-team@cisco.com.

Note If you are a network administrator and need personal technical assistance with a Cisco product that is under warranty or covered by a maintenance contract, contact Cisco's Technical Assistance Center (TAC) at 800 553-2447, 408 526-7209, or tac@cisco.com. To obtain general information about Cisco Systems, Cisco products, or upgrades, contact 800 553-6387, 408 526-7208, or cs-rep@cisco.com.

Documentation CD-ROM

Cisco documentation and additional literature are available in a CD-ROM package, which package that ships with your product. The Documentation CD-ROM, a member of the Cisco Connection Family, is updated monthly. Therefore, it might be more current than printed documentation. To order additional copies of the Documentation CD-ROM, contact your local sales representative or call customer service. The CD-ROM package is available as a single package or as an annual subscription. You can also access Cisco documentation on the World Wide Web at http://www.cisco.com, http://www-china.cisco.com, or http://www-europe.cisco.com.

If you are reading Cisco product documentation on the World Wide Web, you can submit comments electronically. Click **Feedback** in the toolbar and select **Documentation**. After you complete the form, click **Submit** to send it to Cisco. We appreciate your comments.

This document is to be used in conjunction with the documents listed in the "Related Documentation" section on page 35.

Access Registrar, AccessPath, Any to Any, AtmDirector, CCDA, CCDE, CCDP, CCIE, CCNA, CCNP, CCSI, CD-PAC, the Cisco logo, Cisco Certified Internetwork Expert logo, *CiscoLink*, the Cisco Management Connection logo, the Cisco Net*Works* logo, the Cisco Powered Network logo, Cisco Systems Capital, the Cisco Systems Capital logo, Cisco Systems Networking Academy, the Cisco Technologies logo, ControlStream, Fast Step, FireRunner, GigaStack, IGX, JumpStart, Kernel Proxy, MGX, Natural Network Viewer, NetSonar, Network Registrar, *Packet*, PIX, Point and Click Internetworking, Policy Builder, Precept, RouteStream, Secure Script, ServiceWay, SlideCast, SMARTnet, StreamView, *The Cell*, TrafficDirector, TransPath, ViewRunner, VirtualStream, VisionWay, VlanDirector, Workgroup Director, and Workgroup Stack are trademarks; Changing the Way We Work, Live, Play, and Learn, Empowering the Internet Generation, The Internet Economy, and The New Internet Economy are service marks; and Asist, BPX, Catalyst, Cisco, Cisco IOS, the Cisco IOS logo, Cisco Systems, the Cisco Systems logo, the Cisco Systems Cisco Press logo, Enterprise/Solver, EtherChannel, EtherSwitch, FastHub, FastLink, FastPAD, FastSwitch, IOS, IP/TV, IPX, LightStream, LightSwitch, MICA, NetRanger, Registrar, StrataView Plus, Stratm, Telerouter, and VCO are registered trademarks of Cisco Systems, Inc. in the U.S. and certain other countries. All other trademarks mentioned in this document are the property of their respective owners. (9903b R)

Copyright © 1999, Cisco Systems, Inc.
All rights reserved.